

Forum:[Hack Forums](#)

Thread: [Fifty-Fifty.Casino Concerns & Answers](#)

JuicyProgramming - November 2, 2019, 1:45 pm

Dear HF friends,

Since there are a lot of concerns regarding the platform <https://fifty-fifty.casino> - <https://hackforums.net/showthread.php?tid=6009725> as seen here: <https://hackforums.net/showthread.php?tid=6021415>

I feel the need to create this thread to clear up the concerns people have. Please note that this thread will be updated regularly.

C: You have 0% house edge how do you sustain this platform?

A: This platform will be funded mainly by us. The only costs we have is server costs. We do have the option to donate to us and we do not exclude the idea to add ads later on when the server-costs are too high.

C: How do I know that the RNG is fair?

A: Our RNG for both Player vs. Player and Player vs. House is a 100% waterproof. Anyone who says it is not does not understand it. All our info about our RNG can be found on: <https://fifty-fifty.casino/RNG> if someone wants some assistance with understanding it. Kindly send me a PM.

C: Free faucets and Player vs House and 0% edge is impossible!

A: We give free small faucets so people can explore the platform. The Player vs. House is limited to 0.20\$ per bet and has a limit of bets per hour. The amount of which we can lose is also limited so we can never lose more than we want to, and if we lost that amount, it would not be possible to play against the house until we fund the system again. We've implemented Player vs. House so people have something to do on the platform whilst they wait for people to come online. This feature will later be removed.

C: The development is alot of work, how do you fund this?

A: The platform is fully developed by us. We do this as a hobby and all have regular good-paying jobs. The development costs are 0.00\$.

C: You dont have a license and are not registered (and thus you are not legal)!

A: We are non-profit. As stated above we pay the server costs ourself but we are not able to invest the amount needed for a license. We are not able to get investors because we are not making any money out of this. If someone is so generous to funds us the license we will be happy to accept it and officially register the platform. We've had contact with Casino Licensing companies all around the world and a license is NOT required for us (however it would ofcourse be better to have one).

If there are any more concerns I will be happy to clear them up for you.

Thanks for reading and have a wonderful day!

RUMRUN - November 2, 2019, 3:23 pm

It's a scam. This man is a conman. Details submitted to multiple agencies. Attempts to bring up highly technical terms but misattributes them to fit his security narrative.

Ask any credible programmer to verify what he is typing makes sense. The answer is: NO

Main problem: win odds can be rigged at will (goes entirely against the edge claim)

Why? PHP is used to handle the final decision process, PHP is server-side only and not verifiable for the player.

How do credible gambling sites do it (ie bustabit)? They use javascript.

But the client seeds? A cool trick, doesn't do anything odds-wise, you submit everything to the PHP script.

JuicyProgramming - November 2, 2019, 3:56 pm

(Nov 2, 2019 03:23 PM)RUMRUN Wrote: [\[CITE\]](#) It's a scam. This man is a conman. Details submitted to multiple agencies. Attempts to bring up highly technical terms but misattributes them to fit his security narrative.

Ask any credible programmer to verify what he is typing makes sense. The answer is: NO

Main problem: win odds can be rigged at will (goes entirely against the edge claim)

Why? PHP is used to handle the final decision process, PHP is server-side only and not verifiable for the player.

How do credible gambling sites do it (ie bustabit)? They use javascript.

But the client seeds? A cool trick, doesn't do anything odds-wise, you submit everything to the PHP script.

You don't understand our RNG. What you state is wrong, and you can verify that. Please read:

<https://www.fifty-fifty.casino/RNG>

Doesnt matter that we use PHP and you would understand that if you'd read that page.

Besides that, I offered you to explain it and show a demo and you ignored me. Says enough amigo:

<https://imgur.com/a/y0lIR16>

I can not take you seriously anymore.

Rake - November 2, 2019, 3:57 pm

(Nov 2, 2019 03:23 PM)RUMRUN Wrote: [\[CITE\]](#) It's a scam. This man is a conman. Details submitted to multiple agencies. Attempts to bring up highly technical terms but misattributes them to fit his security narrative.

Ask any credible programmer to verify what he is typing makes sense. The answer is: NO

Main problem: win odds can be rigged at will (goes entirely against the edge claim)

Why? PHP is used to handle the final decision process, PHP is server-side only and not verifiable for the player.

How do credible gambling sites do it (ie bustabit)? They use javascript.

But the client seeds? A cool trick, doesn't do anything odds-wise, you submit everything to the PHP script.

Yeah I spoke with him over Disc.

He uses a lot of technical jargon to try and throw you off. End of the day you submit your client seed in plain text which is all handled server side and can't be verified by the user that the casino didn't manipulate the results.

I'm going to have my buddy dive deep explaining from a programming perspective and

cryptography at that, why this isn't actually truly provably fair when it comes down to it.

Think1st - November 2, 2019, 3:59 pm

(Nov 2, 2019 03:23 PM)RUMRUN Wrote: [\[CITE\]](#) It's a scam. This man is a conman. Details submitted to multiple agencies. Attempts to bring up highly technical terms but misattributes them to fit his security narrative.

Ask any credible programmer to verify what he is typing makes sense. The answer is: NO

Main problem: win odds can be rigged at will (goes entirely against the edge claim)

Why? PHP is used to handle the final decision process, PHP is server-side only and not verifiable for the player.

How do credible gambling sites do it (ie bustabit)? They use javascript.

But the client seeds? A cool trick, doesn't do anything odds-wise, you submit everything to the PHP script.

thanks for the info

but kids never gamble

JuicyProgramming - November 2, 2019, 4:00 pm

(Nov 2, 2019 03:57 PM)Rake Wrote: [\[CITE\]](#) Yeah I spoke with him over Disc.

He uses a lot of technical jargon to try and throw you off. End of the day you submit your client seed in plain text which is all handled server side and can't be verified by the user that the casino didn't manipulate the results.

I'm going to have my buddy dive deep explaining from a programming perspective and cryptography at that, why this isn't actually truly provably fair when it comes down to it.

You dont submit your client-seed in plain-text. Please read the RNG page and watch the video. You also ignored me after I explained it. Proof: <https://imgur.com/a/x36N4B4>

Why ya'll telling its not correct but only coming with FALSE INFORMATION.

RUMRUN - November 2, 2019, 5:28 pm

You're the one who has to prove something. Not claim things which are inherently FALSE INFORMATION and MISATtribution OF SECURITY FEATURES.

Yeah. It actually matters that you use PHP. Nobody can verify jack shit.

JuicyProgramming - November 2, 2019, 5:32 pm

(Nov 2, 2019 05:28 PM)RUMRUN Wrote: [\[CITE\]](#) You're the one who has to prove something. Not claim things which are inherently FALSE INFORMATION and MISATtribution OF SECURITY FEATURES.

Yeah. It actually matters that you use PHP. Nobody can verify jack Clay Davis.

You can. Because BEFORE you send your client-seed in plain-text to the server (so BEFORE PHP is used), you see the opponent his client-seed-hash and server-seed-hash and thus confirm AFTER the bet that those where not based upon your client-seed.

The bet is calculated with 3 factors A, B and C

If you know the hashes of B and C before you input A we could've never influenced the outcome based upon your client-seed.

This completely tackles your claim. Again our RNG is 100% waterproof!

crypt - November 2, 2019, 5:37 pm

I deposited and it hit 3 confs but I have not been credited.

Username: cryptotalty

TXID:

<https://blockchair.com/bitcoin/transaction/298cce99521f2b09ae4a79872c45d3bc2ab0004fc31ec2a192402d583124ff35>

Rake - November 2, 2019, 5:45 pm

(Nov 2, 2019 05:37 PM)RUMRUN Wrote: [\[CITE\]](#) Yeah. So what does that fuc.k.ing client seed actually matter if you handle the hashes completely hidden from all public view? You fu.cking retard. For all I care your script just passes the client seeds and does something different out of side, in fuc.king PHP, where it's hidden. Faggo.t.

They scammed a user btw

(Nov 2, 2019 05:37 PM)cryptotalty Wrote: [\[CITE\]](#) I deposited and it hit 3 confs but I have not been credited.

Username: cryptotalty

TXID:

<https://blockchair.com/bitcoin/transaction/298cce99521f2b09ae4a79872c45d3bc2ab0004fc31ec2a192402d583124ff35>

JuicyProgramming - November 2, 2019, 6:14 pm

(Nov 2, 2019 05:45 PM)Rake Wrote: [\[CITE\]](#) They scammed a user btw

No, our cron-jobs of payment verification has been set to 5 minutes currently. More info about cron jobs: <https://en.m.wikipedia.org/wiki/Cron>

We will decrease this as it might cause confusion :)

(Nov 2, 2019 05:37 PM)RUMRUN Wrote: [\[CITE\]](#) Yeah. So what does that fuc.k.ing client seed actually matter if you handle the hashes completely hidden from all public view? You fu.cking retard. For all I care your script just passes the client seeds and does something different out of side, in fuc.king PHP, where it's hidden. Faggo.t.

Nope it is hashed using Javascript inside your computer. It is not hashed on the server. Hopefully that clears it up :)

Anzee - November 2, 2019, 6:55 pm

Fix your website. It's down.

<https://check-host.net/check-report/b4d0986kec1>

I have active bets...

Omniscient - November 2, 2019, 6:59 pm

My opinion on this is that scammers usually don't offer full explanations like this.

<https://fifty-fifty.casino/RNG>

I haven't seen anyone try to confirm their method is valid as provably fair. If you want to claim they are scamming then get proof.

btw, looks like their site under DDOS attack as it's offline. Shame you guys have to be assholes.

Here is there RNG page...

JuicyProgramming - November 2, 2019, 7:12 pm

(Nov 2, 2019 06:55 PM)Anzee Wrote: [\[CITE\]](#) Fix your website. It's down.

<https://check-host.net/check-report/b4d0986kec1>

I have active bets...

Not possible, bets require you to be online. I guess we have our suspect #1 ? Do whatever you wish my friend. Spend your money on us ?

(Nov 2, 2019 06:59 PM)Omniscient Wrote: [\[CITE\]](#) My opinion on this is that scammers usually don't offer full explanations like this.

<https://fifty-fifty.casino/RNG>

I haven't seen anyone try to confirm their method is valid as provably fair. If you want to claim they are scamming then get proof.

btw, looks like their site under DDOS attack as it's offline. Shame you guys have to be assholes.

Here is there RNG page...

I greatly appreciate this comment. And indeed, unfortunately some people have to be assholes but there is nothing we can do about it.

Kill Joy - November 2, 2019, 7:14 pm

I need to test the actual seed generation myself, but the two people attacking this website seem like idiots.

The RNG page covers everything you need to know in great depth. They even went as far as to making sure a user cannot maliciously alter the client-sided seed.

The formulas work out. It seems near similar to how bitcoin addresses are generated as

$(\text{private} + \text{private}) * G = (\text{public} + \text{public})$

Rake - November 2, 2019, 7:24 pm

(Nov 2, 2019 07:14 PM)Kill Joy Wrote: [\[CITE\]](#) I need to test the actual seed generation myself, but the two people attacking this website seem like idiots.

The RNG page covers everything you need to know in great depth. They even went as far as to making sure a user cannot maliciously alter the client-sided seed.

The formulas work out. It seems near similar to how bitcoin addresses are generated as

$(\text{private} + \text{private}) * G = (\text{public} + \text{public})$

Let me know what you find, I'll retract my claims regarding their provable fairness and apologize if you can vouch for their end.

I lack the technical knowledge to fully 100% understand how their methodology works (or at least not

without reading it 4+ times)

So someone more trusted and known explaining or confirming it's legitimate would be appreciated.

Kill Joy - November 2, 2019, 7:30 pm

(Nov 2, 2019 07:24 PM)Rake Wrote: [\[CITE\]](#) Let me know what you find, I'll retract my claims regarding their provable fairness and apologize if you can vouch for their end.

I lack the technical knowledge to fully 100% understand how their methodology works (or at least not without reading it 4+ times)

So someone more trusted and known explaining or confirming it's legitimate would be appreciated.

I'm glad you admit you are not knowledgeable enough to understand their claims; however, you should be ashamed of yourself for your then baseless accusations.

Rake - November 2, 2019, 7:34 pm

(Nov 2, 2019 07:30 PM)Kill Joy Wrote: [\[CITE\]](#) I'm glad you admit you are not knowledgeable enough to understand their claims; however, you should be ashamed of yourself for your then baseless accusations.

I still 100% stand by my legal stance however.

They're not a licensed site.

Blocking arbitrary ISP's makes no sense as they aren't running out of a country which requires them to do so.

So acting as if for example they are licensed outside curacao and blocking the US, and other regions, is completely useless as they lack the proper IP and licensing to begin with.

The owner is right, licensing is expensive, however it's not \$30k expensive. It's still not an excuse to avoid it and run it illegal though

Most allow you to make biannual payments, and it's about \$5k pay payment (\$10K per year , + additional costs such as the business registration, application fees, no more then \$15k total)

Anzee - November 2, 2019, 7:47 pm

(Nov 2, 2019 07:12 PM)JuicyProgramming Wrote: [\[CITE\]](#) Not possible, bets require you to be online. I guess we have our suspect #1 ? Do whatever you wish my friend. Spend your money on us ?

I greatly appreciate this comment. And indeed, unfortunately some people have to be assholes but there is nothing we can do about it.

How can I be online if your site is offline..?

JuicyProgramming - November 2, 2019, 7:55 pm

(Nov 2, 2019 07:47 PM)Anzee Wrote: [\[CITE\]](#) How can I be online if your site is offline..?

Quote:I have active bets...

You cant have active bets. If you create a bet you need to be online and in the lobby. Else your bet will be canceled. You are clearly never used our platform.

(Nov 2, 2019 07:14 PM)Kill Joy Wrote: [\[CITE\]](#) I need to test the actual seed generation myself, but the two people attacking this website seem like idiots.

The RNG page covers everything you need to know in great depth. They even went as far as to making sure a user cannot maliciously alter the client-sided seed.

The formulas work out. It seems near similar to how bitcoin addresses are generated as

$(\text{private} + \text{private}) * G = (\text{public} + \text{public})$

Thanks alot for the kind reaction. I truely appreciate it. If there is something we can improve, let us

know and we will fix things as soon as we can.

SIM-4086413 - November 3, 2019, 1:31 am

(Nov 2, 2019 07:24 PM)Rake Wrote: [\[CITE\]](#) I lack the technical knowledge to fully 100% understand how their methodology works (or at least not without reading it 4+ times)

Fucking morron, you have been bashing on these guys for days now while you have no knowledge whatsoever.

You even went to the extend of harrassing these guys which i'll make sure you get reported for as this is a bannable offense.

Fucking baboon

Anzee - November 3, 2019, 2:21 am

I like how Omniscient gave JuicyProgramming a Taco Taco Taco reading "Don't let them get you down." and his site has been returning a "521: Web server is down" error for 8 hours now.

How much downer can you get if not completely?

SIM-4086413 - November 3, 2019, 2:37 am

(Nov 3, 2019 03:21 AM)Anzee Wrote: [\[CITE\]](#) I like how Omniscient gave JuicyProgramming a Taco Taco Taco reading "Don't let them get you down." and his site has been returning a "521: Web server is down"error for 8 hours now.

How much downer can you get if not completely?

As omni said his site is under a ddos attack most likely, and i won't be surprised if Rake is behind it.

JuicyProgramming - November 3, 2019, 4:29 am

(Nov 3, 2019 03:37 AM)Magaddino Wrote: [\[CITE\]](#) As omni said his site is under a ddos attack most likely, and i won't be surprised if Rake is behind it.

We are fixing some things as we speak. Should be back up shortly.

Omniscient - November 3, 2019, 9:44 am

Quote:I still 100% stand by my legal stance however.

They're not a licensed site.

Then make that claim and stand by it. Don't make claims that are BS just to make your argument look better. If I was in a less forgiving mood you might have been closed.

As for the whole unlicensed/illegal claim. Are you sure that even matters to the HF crowd? And the fact is that running a Curacao licensed gambling site doesn't suddenly make you legal. The legal/illegal aspect only really pertains to them as a business and how it legally effects them. And you can be 100% licensed and fully legal in Curacao but then still be illegal in USA. That's sort of my point. Just doesn't matter imho that much. It's not the deal breaker. Lots of these gambling sites are shady when it comes to legalities.

Take Bustabit for example. The words "legal" or "licensed" is nowhere to be found on their site. I just rarely see these Bitcoin gambling sites touting how legal they are.

Last point too on that licensed/legal crap...the site Liberty Reserve was licensed and legal too. Until it wasn't.

I think gamblers know the risk of depositing into these sites. It's up to the site to earn trust but you

don't have to make it harder by making false and malicious claims.

Quote:We are fixing some things as we speak. Should be back up shortly.

You have to protect against DDOS sooner or later anyways.

Butter - November 3, 2019, 10:18 am

If the codes not opensource, I don't hame the private keys and the project is not decentralised..

Spoiler ([Click to View](#))

...I'm out

Omniscient - November 3, 2019, 10:25 am

(Nov 3, 2019 11:18 AM)Butter Wrote: [\[CITE\]](#) If the codes not opensource, I don't hame the private keys and the project is not decentralised..

Spoiler ([Click to View](#))

...I'm out

That's a reasonable decision to make.

I wouldn't opensource my custom code. Fuck that. By releasing it you will create clones and competition.

And if you have their private key that's a security risk. Maybe you mean your own private key? Decentralized is nice though. Maybe they will add that once their site is more established.

Rake - November 3, 2019, 10:33 am

(Nov 3, 2019 10:44 AM)Omniscient Wrote: [\[CITE\]](#) Then make that claim and stand by it. Don't make claims that are BS just to make your argument look better. If I was in a less forgiving mood you might have been closed.

As for the whole unlicensed/illegal claim. Are you sure that even matters to the HF crowd? And the fact is that running a Curacao licensed gambling site doesn't suddenly make you legal. The legal/illegal aspect only really pertains to them as a business and how it legally effects them. And you can be 100% licensed and fully legal in Curacao but then still be illegal in USA. That's sort of my point. Just doesn't matter imho that much. It's not the deal breaker. Lots of these gambling sites are shady when it comes to legalities.

Take Bustabit for example. The words "legal" or "licensed" is nowhere to be found on their site. I just rarely see these Bitcoin gambling sites touting how legal they are.

Last point too on that licensed/legal crap...the site Liberty Reserve was licensed and legal too. Until it wasn't.

I think gamblers know the risk of depositing into these sites. It's up to the site to earn trust but you don't have to make it harder by making false and malicious claims.

You have to protect against DDOS sooner or later anyways.

You know they're not just advertising to the "HF Crowd" ?

They've also got a Bitcointalk post with more pages , traction, then this HF one where they were ridiculed for not having a license as well.

A curacao license and registered business there does actually make you legal in fact, however you're still required to block certain regions jurisdictions such as the USA.

If you're running a completely unlicsend site, i.e not even curacao, almost now jurisdiction allows the use of your platform, and it gets even more fuckery when you start cashing out the profits to fiat and have to explain where it came from.

Glad you mentioned bustabit, they do mention they're licesned if you ask anyone or the owner in the chat.

<https://www.bustabit.com/>

Scroll to the bottom, it's stamped on their site, they are indeed licensed out of curacao and operate under the business "Apis N.V" there

Natas - November 3, 2019, 10:42 am

No hate at all [Rake](#) but this seems dramatic to me ...

I sense some jealousy since you have a btc gambling as well ?

Omniscient - November 3, 2019, 10:43 am

Quote:They've also got a Bitcointalk post with more pages

Convo me the link to it please. Have not found it via their shitty search.

Quote:A curacao license and registered business there does actually make you legal in fact

lol...that's funny.

Quote:however you're still required to block certain regions jurisdictions such as the USA.

Then why doesn't Bustabit block US region IPs?

You're kind of stupid Rake. Unsure why, maybe you just have never run a business or something. And more or less everyone knows you're attacking the site. So you speak about legal shit then DDOS a site because you're an asshole.

Say bye bye.

Fifty-Fifty - November 3, 2019, 11:58 am

First of all, i would like to say a big thank you to Omniscient and Kill Joy for clearing this mess up.

And i hope Rake and Rumrun learned there lesson, when it comes to making accusations based on assumptions.

Second i would like to add something on the legal aspect.

A licensed casino could operate illegally, if they offer games of chance to a Jurisdiction in which it is illegal to gamble online.

Other other way around. An unlicensed casino that uses cryptocurrency(which is not accepted as a currency by most nations) is not operating illegally if they do not offer games of chance to their users. After we start blocking IP addresses we will be operating in a so called "grey area" where we are not illegal nor officially legal.

And guys, if there is anything you would like see added to the platform let us know! We will be

listening to all feedback good or bad. It's not only our platform but yours as well, tell us we make it! :)

Have a wonderful day everyone! ?

Kill Joy - November 3, 2019, 12:11 pm

(Nov 3, 2019 11:33 AM)Rake Wrote: [\[CITE\]](#) You know they're not just advertising to the "HF Crowd" ?

They've also got a Bitcointalk post with more pages , traction, then this HF one where they were ridiculed for not having a license as well.

A curacao license and registered business there does actually make you legal in fact, however you're still required to block certain regions jurisdictions such as the USA.

If you're running a completely unlicsend site, i.e not even curacao, almost now jurisdiction allows the use of your platform, and it gets even more fuckery when you start cashing out the profits to fiat and have to explain where it came from.

Glad you mentioned bustabit, they do mention they're licesned if you ask anyone or the owner in the chat.

<https://www.bustabit.com/>

Scroll to the bottom, it's stamped on their site, they are indeed licensed out of curacao and operate under the business "Apis N.V" there

There is nothing indexed for the casino besides their website and one of these threads.

Way to waste a few hours of people's time altogether.

MavenGradle - November 3, 2019, 12:31 pm

Quote:Another property of hashing is that it is impossible to find 2 different inputs with the same output

This is completely wrong and not at all true. If you knew a thing or two about hashing and probability calculations you would realise that it is actually IMPOSSIBLE to always generate unique fixed length strings using an infinite number of possible inputs. This has a name by the way. It's called a hashing collision:

[https://en.wikipedia.org/wiki/Collision_\(computer_science\)](https://en.wikipedia.org/wiki/Collision_(computer_science))

I stopped reading after that because that's just one of the basics surrounding hashing.

(Nov 2, 2019 04:00 PM)JuicyProgramming Wrote: [\[CITE\]](#) Why ya'll telling its not correct but only coming with FALSE INFORMATION.

I have no affiliation with the user you quoted but if anything, my text alone is reason to believe that you are spreading false information. Provable false information even. Perhaps you should consider changing your RNG explanation to reflect the proper data.

Other than that I do not call your company a scam or anything of the sort, but you should really update your data. This just looks very unprofessional. I hope you realise that collision attacks are very much a thing that you should not take lightly:

https://en.wikipedia.org/wiki/Collision_attack

Fifty-Fifty - November 3, 2019, 1:04 pm

(Nov 3, 2019 01:31 PM)MavenGradle Wrote: [\[CITE\]](#) This is completely wrong and not at all true. If you knew a thing or two about hashing and probability calculations you would realise that it is actually IMPOSSIBLE to always generate unique fixed length strings using an infinite number of

possible inputs. This has a name by the way. It's called a hashing collision:

[https://en.wikipedia.org/wiki/Collision_\(computer_science\)](https://en.wikipedia.org/wiki/Collision_(computer_science))

I stopped reading after that because that's just one of the basics surrounding hashing.

I have no affiliation with the user you quoted but if anything, my text alone is reason to believe that you are spreading false information. Provably false information even. Perhaps you should consider changing your RNG explanation to reflect the proper data.

Other than that I do not call your company a scam or anything of the sort, but you should really update your data. This just looks very unprofessional. I hope you realise that collision attacks are very much a thing that you should not take lightly:

https://en.wikipedia.org/wiki/Collision_attack

It's indeed not 'impossible'. But finding such a collision can take an extremely, extremely long time! For the server-seed-hash(which is a hash of a random 256 bit number), it is nearly impossible to find a collision. This could take up billions of years. Regarding the client-seed, the client-seed has a maximum length of 20 characters. So you would have to find a collision with only 20 characters and that is even less likely.

You are absolutely 100% right and we will update our RNG page soon regarding this. We appreciate the heads up! :)

But did you ever find a SHA-256 collision, or has there ever been found one? :\$

For now we chose to use SHA-256, in the future we will upgrade to SHA-512 to make it even more secure.

We really appreciate your feedback, thanks. If there is anything else please let us know! :)

Kill Joy - November 3, 2019, 2:32 pm

(Nov 3, 2019 02:04 PM)Fifty-Fifty Wrote: [\[CITE\]](#) It's indeed not 'impossible'. But finding such a collision can take an extremely, extremely long time!

For the server-seed-hash(which is a hash of a random 256 bit number), it is nearly impossible to find a collision. This could take up billions of years. Regarding the client-seed, the client-seed has a maximum length of 20 characters. So you would have to find a collision with only 20 characters and that is even less likely.

You are absolutely 100% right and we will update our RNG page soon regarding this. We appreciate the heads up! :)

But did you ever find a SHA-256 collision, or has there ever been found one? :\$

For now we chose to use SHA-256, in the future we will upgrade to SHA-512 to make it even more secure.

We really appreciate your feedback, thanks. If there is anything else please let us know! :)

Collisions, at least in Bitcoin (SHA-256), have been found only after massive computing power or due to bad RNG values. The collisions still only happened mainly due in part to following a known pattern.

Fifty-Fifty - November 8, 2019, 12:35 pm

(Nov 3, 2019 01:31 PM)MavenGradle Wrote: [\[CITE\]](#) This is completely wrong and not at all true. If

you knew a thing or two about hashing and probability calculations you would realise that it is actually IMPOSSIBLE to always generate unique fixed length strings using an infinite number of possible inputs. This has a name by the way. It's called a hashing collision:

[https://en.wikipedia.org/wiki/Collision_\(computer_science\)](https://en.wikipedia.org/wiki/Collision_(computer_science))

I stopped reading after that because that's just one of the basics surrounding hashing.

I have no affiliation with the user you quoted but if anything, my text alone is reason to believe that you are spreading false information. Provable false information even. Perhaps you should consider changing your RNG explanation to reflect the proper data.

Other than that I do not call your company a scam or anything of the sort, but you should really update your data. This just looks very unprofessional. I hope you realise that collision attacks are very much a thing that you should not take lightly:

https://en.wikipedia.org/wiki/Collision_attack

We made a disclaimer at the bottom of our RNG page. :)

Again, thank you for the heads up!

Fifty-Fifty.casino/RNG

LordMan - November 8, 2019, 1:24 pm

I agree with Omniscient that these guys appear trustworthy. I know from Dutch people, in general, they are serious people.

I'm not shy to try playing a few of micro-stakes games on their website. Although, I think you need some sort of GLI certification to actually legally run or promote a business like this by the way. How are you going to reach new players? I think you will gain more trust from your visitors if you show the replay or at least the results of the recently played games. But that's just the start of your journey. Investing in your business and networking with other parties is mandatory to get the desired hits per day. Stay realistic because probably less than a quarter % of your unique visitors will follow to play.

My advice is to be active in related communities. But that requires a lot of time and of course fluent English. Like not mine obviously. I personally would recruit content writers who manage social media and other communities

Fifty-Fifty - November 8, 2019, 2:18 pm

(Nov 8, 2019 02:24 PM)LordMan Wrote: [\[CITE\]](#) I agree with Omniscient that these guys appear trustworthy. I know from Dutch people, in general, they are serious people.

I'm not shy to try playing a few of micro-stakes games on their website. Although, I think you need some sort of GLI certification to actually legally run or promote a business like this by the way. How are you going to reach new players? I think you will gain more trust from your visitors if you show the replay or at least the results of the recently played games. But that's just the start of your journey. Investing in your business and networking with other parties is mandatory to get the desired hits per day. Stay realistic because probably less than a quarter % of your unique visitors will follow to play.

My advice is to be active in related communities. But that requires a lot of time and of course fluent English. Like not mine obviously. I personally would recruit content writers who manage social media and other communities

Well to start off; Thank you for having faith in us! :)

We would like to see word of mouth advertisement but ofcourse, we can't ask for that. So we are thinking about adding a referral program.

Once you played a bet the results are saved! You can check your bet history at "my bets" and also verify then when ever you feel like.

Only small part of our unique visitor play. We are not able to list the platform in any affiliate programs due to not being licensed...

We try to be as active as possible but do not forget we don't do this full-time. We will be continuously working on improving the platform and if gamblers do want to lose their funds to any company or casino, its their choice. :)